

1 Introduction

1.1 Problem Summary

Problem Statement

Despite the existence of many cyber security awareness programs, there is still a lack of effective, widespread cyber security training

As modern-day technology is ever evolving, the number of users who interact with technology on a daily basis increases consequently. As a result, the risk of an individual, or business, becoming a victim to cyber-crime increases proportionately. In particular, small and medium-sized businesses (SMBs) are the biggest sectors targeted by cyber-criminals [1], which stem from issues such as budget restraints and expressing a lack of understanding towards cyber security concepts.

In fact, as a consequence of COVID-19 changing the dynamic of industry standards this year, a statistical analysis from May 2020 (UK) showed that individuals experiencing targeted hacking increased by 77.41% - in comparison with the previous year [2]. This is most likely due to the fact that employees are encouraged to work from home via their personal computers. Consequently, this has fed into a new strategy whereby cyber-criminals are moving laterally into organisational infrastructure by targeting and infecting employees at their less secure personal computers [3].

In regards to this problem, this paper will explore the effectiveness of educational games - which has been shown to have an advantage on the learning outcome in comparison with traditional training material [4]. Therefore, this paper presents the following research question and hypothesis:

Research Question

Does teaching cyber security through a gamified medium improve user confidence in protecting against cyber attacks?

Hypothesis

Creating an educational cyber security game will leave users feeling more confident and aware with regards to cyber security concepts

1.2 Goals & Scope

The goal of this project is to investigate how to effectively apply gamification mechanics in order to teach cyber security principles appropriately. The expected result of this project is to create a multiplayer, online tabletop board game.

2 Literature Review & Research

2.1 Introduction

To date, this report includes an evaluation of literature review pertaining to pre-existing cyber security games, mechanics for game-based learning and current trends in cyber security training methodologies.

2.2 The Problem with Current Cyber Security Training Programs

This report will specifically analyse the shortcomings and difficulties that relate to current training programs designed for small and medium-sized businesses [1, 5].

Problem	Description
1	SMBs can be heavily constrained by a limited budget
2	SMBs can be difficult to reach as they do not understand the severity of data breaches
3	SMBs are often distracted by the operational requirements for setting up and running a small business
4	SMBs struggle to identify their assets in terms of the risks associated with them

In regards to the delivery of training programs, providing generalised cyber security advice (from an independent advisor) has been shown to have little effect on changing the behaviour of employees within SMBs [1, 6]. Furthermore, traditional training simulations (including gamified video simulations) are generally undertaken in a formal environment which leads to a situation of recipients not absorbing the information well [2].

The methodology of cyber security exposure is also important as whilst employees may understand some general information about the vulnerability demonstrated, they may still fail to see how it relates to their workplace environment [5] or how they link together in a multifaceted social engineering attack [6]. This last point emphasises the need for widespread conceptual training in cyber security.

2.3 A Critical Analysis of Pre-Existing Cyber Security Games

For a full account of educational games and resources reviewed, please see Appendix A. My methodology for reviewing cyber security games was two fold:

- First - utilising the Google search engine with the following keywords: ‘cyber security’, ‘serious games’, ‘gamification’ and ‘game-based learning’ in order to look for any widely available games. These commonly returned web applications designed for students in all stages of education.

- Second - utilising Google Scholar and the IEEE Database with similar keywords in order to find academic papers which either reviewed other educational games, or were proposing one. For the games that were not available online, I summarised the key information and research results from the academic source material.

Building on from this, I concluded the following categories of educational game-based learning strategies in order to identify the most appropriate medium for the purpose of answering the research question and hypothesis established in this project.

2.3.1 Web Applications

Advantages	Disadvantages
Simple point and click interactivity	Can lack depth and relevance to a specific target (often designed for students)
Easily accessible anywhere with an internet connection	Not suitable for offline usage
Cheap development cost & time	

2.3.2 Video / Simulation

Advantages	Disadvantages
Contextually appropriate for use within the workplace [5]	Not appropriate for the general public & students
Accessible both online & offline	Requires multiple play-throughs if scenarios are divergent
	Typically not very fun as undertaken in a formal environment [5]

2.3.3 Cooperative Tabletop

Advantages	Disadvantages
Encourages social engagement and team-working	Requires multiple players
Cheap to prototype and produce a physical implementation	Requires much fine-tuning of rules and mechanics implemented
Encourages thinking strategically	

2.3.4 Task Management

Advantages	Disadvantages
Easy to employ around current learning strategies (within the classroom or workplace)	Requires long term evaluation of effectiveness
Perfect example of procedural learning [7]	Not a true application of an educational game

2.3.5 Single Player

Advantages	Disadvantages
Immersive and engaging typically through story driven content	High development cost & time
Often places the player as a white / black hat hacker which encourages adversarial thinking	Lack of exploration on how to prevent vulnerabilities as a target

2.4 Difficulties that Pre-Existing Cyber Security Games Face

Many of the educational games reviewed relied heavily on presenting facts and then subsequently quizzing the user with a related question. However, users can utilise common sense to rule out incorrect answers thus fail to invoke critical thinking and do not keep the user engaged.

As a solution, gamified strategies should incorporate a variety of factual, conceptual and procedural learning methodologies [7]. In particular, a strong conceptual understanding should be prioritised due to the rapidly changing landscape of cyber security in which cyber-criminals will always be engineering new attack vectors [6]. Therefore, it is imperative for end-users to be able to adapt their way of thinking when interacting with new technology.

For procedural learning, both Nova Cyber Lab [8] and Classcraft [9] (Appendix A) exemplify this by beginning with simple challenges and progressively increasing the difficulty of said challenges as the user progresses. Unlike the other games reviewed, Classcraft is unique as it encourages users within a team to continually expand upon their knowledge by working towards new goals and objectives collaboratively. Furthermore, this system incorporates real-world rewards and punishments to encourage user-engagement.

Finally, many serious cyber security games are designed primarily for university students and businesses but are not readily available to the general public [7]; this agrees with my own research - whereby many of the publicly accessible educational games I reviewed were considerably outdated and not intended for the general public.

2.5 Why Use a Game-Based Learning Approach?

As identified above, many challenges that arise when attempting to educate employees within the business environment occur due the formality of traditional training methodologies in which employees will aim to complete as fast as possible [6]. This absentmindedness often results in training content which is not absorbed effectively [1, 6]. However, these challenges can often be overcome with game-based learning strategies [4].

A summary of key strengths and motivations for gamification [4, 10, 11, 12, 13] include:

- Rapid progress paired with instant feedback
- Strong user engagement
- Allows the user to learn from mistakes in a safe, non punishing environment which would otherwise discourage exploration (due to the fear of failure)
- Serves as a platform to encourage self-learning at the user's desired pace
- Allows the user to become deeply immersed into the 'game - world' where learning feels like a secondary objective
- Relatively cheap and low cost to produce in comparison to larger training schemes
- Requires little to no supervision
- Easy to distribute across multiple platforms and incorporate into the workplace
- Easy to integrate within events such as hackathons and other cyber security awareness gatherings
- Use of an integrated rewards system such as badges, hidden achievements and the desire to win
- Educationally appropriate by incorporating a structure/story that is contextually similar to the real world

2.6 Appropriate Gamification Mechanics

Forde's report [14] identifies the following gamification mechanics in order to increase the adoption rate of effective cyber security standards within the workplace:

- Avatar / User Profile
- Badges / Privileges
- Challenge
- Competition
- Collaboration
- Feedback / Guidance
- Goals / Objectives
- Incentives / Rewards
- Leaderboards
- Points System
- Progress / Levels
- Role Playing
- Story
- Tips / Hints System

2.7 Conclusion

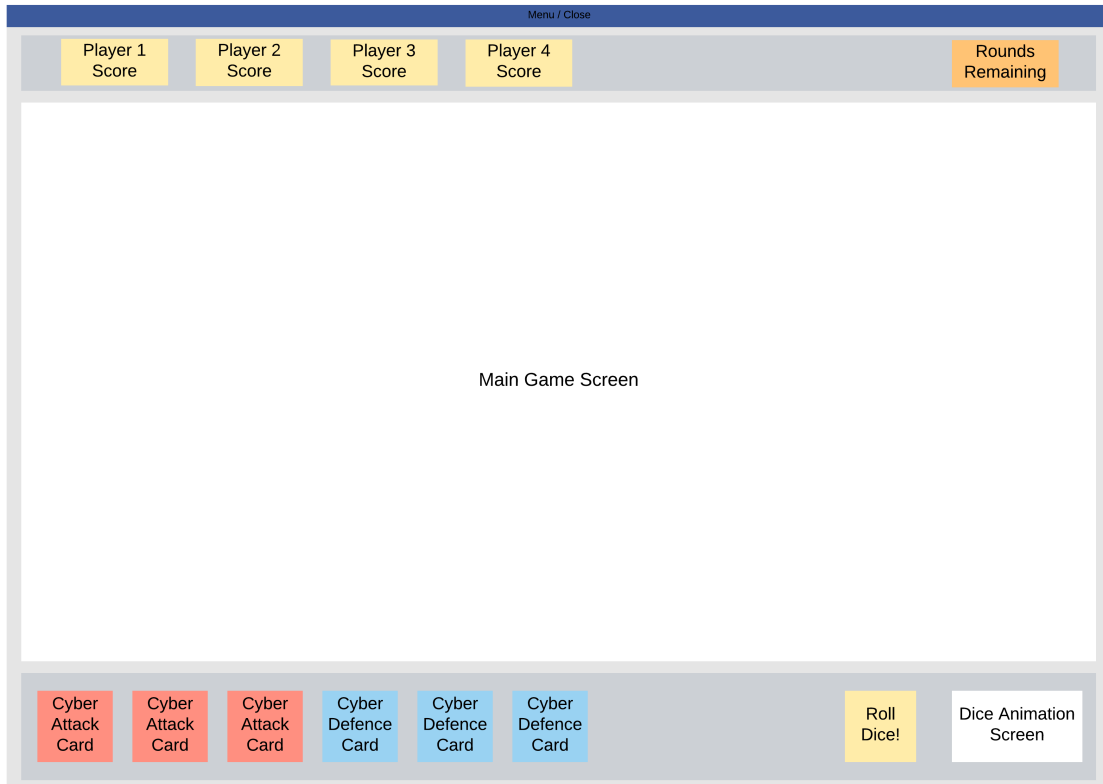
To summarise, cyber security training programs need to be cost effective and target the specific needs and requirements of the workplace in order to be viable for SMBs. Furthermore, where traditional training methodologies fall short, gamified strategies can offer a more cost-effective solution for teaching relevant cyber security concepts. However, unless the game in question has a strong story (e.g. Hacknet [15]), many educational games reviewed included a number of flaws which stem from lack of gamified mechanics that encourage meaningful play. Forde’s report [14] identifies these key mechanics as multiplayer, leaderboards, points system and competition which can be deemed as the most effective in motivating people to participate and learn about a subject that they would otherwise have little interest in. Lastly, there is a gap in the public domain in which an appropriately designed cyber security game could be of use.

3 The Proposed Final Design

3.1 Proposed Idea

The proposed application is a 2-4 multiplier board game. As identified in the literature review, cooperation and competition are two of the most effective mechanics for engaging meaningful game play. The application will be loosely inspired from Mario Party's format, in which players will roll a dice in order to move around tiles on the map. An initial map idea is a typical working office where the goal is to race to navigate towards significant rooms where vulnerabilities are located (such as memory sticks laying around, unattended computers etc). The core game-play will involve collecting these objects and, in the process of moving, players may land on optional item tiles which will drop a defence or attack card respectively; these cards can be used against other players to handicap their movements or score. Finally, between each round, (or if a player lands on a certain tile), a mini-game challenge pertaining to a cyber security concept will be triggered in which the players can compete against each-other.

Figure 1: Wireframe illustrating the Board Game UI



3.2 Functional Requirements

Requirement	Description
Multiplayer	Users are able to play in turns with other users
Web Accessible	Users are able to access the the game lobby from their web browser
Game is Playable	Users are able to play a full version of the game
Account Registration	Users are able to register and login
Save Profile	Users profiles are saved (and earned achievements integrated with MySQL)
Achievements	Users are able to earn achievements from progress
Score / Leaderboard	Users can see their score vs other players
Single Player Mode	Users can play single player (versus computer AI)

3.3 Non - Functional Requirements

Requirement	Description
Availability	The application should be accessible on both desktop web browsers and via mobile tablets
Ease of use	The application should be easy to learn and understand
Accessibility	The application should cater for disabilities such as colour blindness
Security	The application should be secure and protect user's credentials should account registration be implemented
Factually Correct	The application should be factually correct with any cyber security concepts explored
Performance	As a web browser game, it should be relatively smooth to both play and load (with quick multiplayer response times). However, latency is less of an issue given the turn-based mechanic.
Scalability	Should be able to deal with 2-4 connected users per game

3.4 A Brief Account of Work to Date

- Appropriate mechanics have been identified and researched from pre-existing serious cyber security games and literature review
- Appropriate Game Engine (Unity), cloud services (Photon Engine) and APIs have been identified in order to create and host the game
- Cyber security vulnerabilities, game - objects and mini-game ideas for the final implementation have been brainstormed
- A wireframe of the game interface has been mocked up

3.5 A Justification of this Approach

As identified in the literature review, a list of issues identified with pre-existing cyber security games (and comparable training methods) can be justified as follows:

1. Making a publicly available game is both cheap to produce and distribute which meets the budget constraints of SMBs. This also complements the lack of cyber security games available within the public domain
2. A board game with a workplace setting is contextually appropriate for identifying the risks present within SMBs
3. The inclusion of mini-games and vulnerabilities as objectives can be used to explore concepts and trends within cyber security
4. Cyber attack & defence cards encourage the player to consider the perspective of both cyber attackers and themselves (as a potential target to cyber-criminals)
5. Multiplayer is key for encouraging meaningful play as well as overcoming the pitfalls of traditional training methodologies
6. A score board with achievements and objectives encourage competition between players
7. Using a similar rule-set to Mario Party as well as incorporating the identified mechanics in Forde's report [14] reduces the likelihood of developing a game which isn't fun, effective and/or fails to meet the requirements outlined above

4 A Plan of Remaining Work & Project Planning

4.1 Remaining Work

Task / Requirement	MoSCoW	Difficulty
Establish Multiplayer Networking	Must	High
Web Browser Accessible	Should	Medium
Logic for Turn Based Movement	Must	Medium
Add Graphics & Sound Assets	Must	Low
Add Cyber Attack & Defence Items	Must	Low
Add Objectives & Goals	Must	Low
Add Minigame Tiles & Rounds	Should	High
Add a Score / Leaderboard	Should	Low
Account Registration	Could	Medium
Save Profile	Could	Medium
Add Achievements	Could	Low
Test the Application	Could	High
Complete the Application	Must	Very High
Obtain Feedback of Application	Could	Medium
Single Player Mode (with AI)	Won't	Very High

Single player mode is a desirable feature however multiplayer is more appropriate within the context of a board game and meets the requirements of collaboration and competition.

4.2 Project Management Tools & Techniques

Tools	Description
Southampton GitLab	Ability to share a visual representation of tasks completed via GitLab's Boards, Issues and Milestones as well as handle version control
Trello	Visual representation for setting daily & weekly tasks
Workona	Chrome extension for streamlining online research into a succinct workplace
Menderley	Reference management for supporting literature
Google Drive	Cloud storage for research, recording minutes and sharing documents
Unity Engine	Game engine for developing for the Web (WebGL)
Photon	Cloud service for hosting multiplayer servers online
Vagrant	Establishing a virtual software development environment

4.3 Gantt Chart for Phase 1

Week Beginning	1	2	3	4	5	6	7	8	9	10
Date beginning	Oct 5	Oct 12	Oct 19	Oct 26	Nov 2	Nov 9	Nov 16	Nov 23	Nov 30	Dec 7
Planning										
Project Brief										
Literature Review										
Submit Project Brief		x								
Project Planning / Gantt Draft										
Form Hypothesis / Research Question										
Research										
Review Gamemaking Toolkit										
Research Pre-Existing Cyber Security Games										
Research Game Mechanics										
Brain Storm Game										
Research Dev Tools/Languages/APIs										
Write Progress Report										
Submit Report										x

4.4 Gantt Chart for Phase 2

The proposed schedule for semester 2 accounts for a two-week examination period and aims to finish 6 weeks before the deadline (with the final two weeks set by for testing and analysis). Should the project takes more time than anticipated, feedback-testing can be missed.

Week Beginning	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Date beginning	14/12	21/12	28/12	4/1	11/1	18/1	25/1	1/2	8/2	15/2	22/2	1/3	8/3	15/3	22/3	29/3	5/4	12/4	19/4	26/4
Implementation				Exams																
Wireframes of Board/UI																				
Set Up Dev Environment																				
Set Up Multiplayer Networking (Photon)																				
Create Board Outline																				
Turn Based Logic																				
Graphics & Sound Assets																				
Attack & Defence Items																				
Add Objectives & Goal																				
Minigame Tiles / Rounds																				
Score Board																				
Login Authentication																				
Profile & Achievements																				
Testing / Evaluation																				
Write Unity Test Cases																				
Obtain Ethics Approval																				
Obtain Feedback from Playtesters																				
Analyse Feedback																				
Write Final Report																				
Submit Final Report																				x

4.5 Risk Assessment

Risk	Prob (1 - 5)	Severity (1 - 10)	Risk Exposure (P X S)	Mitigation
Project deadlines not met	3	10	30	Weekly meetings with project supervisor to continuously evaluate progress and aspires to finish early in order to provide a buffer period
Not obtaining Ethics Approval in time	3	9	27	Submit identified research questions by no later than mid January
Online Multiplayer not being possible due to limitations/pricing of cloud server hosting	3	8	24	Possibility to incorporate LAN multiplayer functionality by utilising the Unity Mirror API. Failing this, it would suffice to implement multiplayer co-op from the same system
Relevant cyber security principles are not effectively taught	3	7	21	By identifying an appropriate target demographic and the most appropriate cyber security content to teach
Over/under estimating scope of implementation	3	7	21	Aspired project is relatively modular whereby smaller features (identified as Could in the MoSCoW analysis) can be foregone if required. There is also the alternative of implementing Single Player AI instead of multiplayer functionality
Final project doesn't relate to original problem statement/hypothesis	2	9	18	Continuously referring back to the initial problem statement and hypothesis
Sickness / Flu / Mental Health difficulties from Covid19	2	8	16	By exercising daily and reaching out for support earlier (rather than later)
Complications due to Covid19	5	3	15	Aspired project will utilise online multiplayer (for remote gameplay), alongside Microsoft Teams, Discord & GitLab for communication and development
Gamified mechanics are not appropriately utilised	2	7	14	By identifying key mechanics through literature and game review and prioritise the most fundamentally important for this project
Stolen work/data from: cloud storage account being compromised / downloading ransomware	1	10	10	By using randomly generated passwords and 2FA as well as manually backing up important files weekly
Loss of work/data from: PC breaking / Cloud storage servers failing	1	10	10	Storing a copy of work across multiple platforms (Southampton Git, Locally and Google Drive)